Gizlilik ve Güvenlik Rehberi

Rehberi Xeyossr (Discord: @xeyossr , Instagram: @xeyossr) hazırlamıştır. Rehber'de https://guvenlik.oyd.org.tr'den bazı alıntılar var.

Güvenlik Tipi	Bu nedir?	Ne zaman faydalıdır?
Beşeri Güvenlik	**Davranışlarınız** ile ilgili yapabileceğiniz küçük değişiklikler.	İnsan hatalarının bir güvenlik sistemindeki *zayıf halka* olmasını engeller.
Cihaz Güvenliği	**Bilgisayar ve telefonlarınızı** saldırılara daha dayanıklı kılacak adımlar.	Cihazınızın *fiziksel* olarak saldırganların eline geçmesi durumunda bilinen saldırılara karşı dayanıklı kılmak yararlıdır.
Yazışma Güvenliği	**Her mesajı** gönderir veya alırken şifreleme yolları.	Eğer belirli bir mesajın gönderilir ve depolanırken **mahremiyetini** teminat altına almak için gereklidir.
Ağ Güvenliği	Sizi takip eden siteleri engellemek ve **İnternet trafiğinizi** şifrelemek.	Davranışsal takiplere, hesap çalınmalarına, sansüre, sosyal ağ takibine, dinlemlere ve reklamlara karşı korunmaya yardımcı olur.

Mesaj Disiplini

Mesaj Disiplini; Size gelen herhangi bir e-Posta'nın phishing olup olmadığını anlamanıza yarayacaktır.

Gönderene asla güvenmeyin

Yaşanan çoğu saldırının temel kaynağının e-postalar olmasının nedeni gönderenin kimliğini doğrulama imkanı olmamasıdır. Tekrar edelim; Herhangi biri, bir e-postanın gönderen bilgisini başka birinden gelmiş gibi taklit edebilir. Gönderenin doğrulanması zor olduğundan, e-posta kutusu oltalama ve kötücül yazılımlarla yapılan saldırıların habitatıdır.

Oltalama Saldırısı: Bir kişinin olmadığı biri gibi kendini tanıtıp, bu aldatma ile bilgi elde etmesidir. Saldırgan bu yöntem ile kimlik bilgilerinin, bankacılık bilgilerinin, parolaların veya diğer hassas verilerin peşinde olabilir.

Kötücül yazılım saldırısı: Bir saldırganın sizi, bilgisayarınıza bir bağlantı veya eklenti aracılığı ile kötücül bir yazılımı yüklemeniz için kandırmasıdır.

Genel olarak e-posta kutunuzda gördüğünüz beklenmedik her e-postaya şüpheyle yaklaşmalısınız. Sizden bir bağlantıya tıklamanızı, bir eklentiyi indirmenizi veya bir bilgiyi göndermek gibi bir şey yapmanızı isteyen her e-posta -tanıdığınız birinden bile olsa- şüphe uyandırmalıdır. Eğer hesabınıza başka biri tarafından girildiyse; hatırlamadığınız yanıtlar, yeni girdiler, yeni dizinler, oluşturmadığınız filtreler veya ayarlarınızda değişiklikler görmeniz mümkündür. Bunun gibi şüpheli durumlarda teknik destek almalı ve önleyici bir çözüm olarak parolalarınızı değiştirmelisiniz.

E-postalardaki bağlantılardan sakının

Bağlantılar (linkler), çoğunlukla masum görünümlü, hatta kimi zaman e-postanın içinde gizli olan, saldırganların sizden bilgi çalmalarının veya cihazlarınızı ele geçirmelerinin en yaygın yollarından biridir. En iyisi, e-postalarla gelen bağlantılara asla tıklamamaktır. Eğer e-posta ile gelen bir bağlantının mutlaka açılması gerekiyorsa şunlara dikkat edilmelidir:

- E-posta bekliyor muydunuz? Gelen adres tanıdığınız birinden gibi görünse bile, beklemediğiniz e-postalara dikkatle yaklaşmakta fayda vardır.

- Gelen bağlantıya tıklamak yerine elle yazabilir misiniz? Gönderilen bağlantı göründüğü gibi olmayabilir. Alan adları, aslına benzer eşyazımlar veya farklı harfler içeriyor olabilir (Ör. rakam olan "0" ile büyük "O", veya Latin ile Kiril alfabesi gibi). Size gelen bağlantı, https://discord.com gibi görünüyor olabilir fakat aslında sizi saldırganın web sitesi olan https://discord.com adresine yönlendiriyor olabilir (İkinci bağlantıda Yunan alfabesindeki

"o/omicron" harfi var.). Bu tip saldırıları önlemenin en güvenli yolu, ilgili bağlantıyı adres çubuğuna elle yazmaktır.

- Alan adını tanıyor musunuz? Çoğu e-posta istemcisi, web tarayıcılarında olduğu gibi, imleci bağlantıların üzerinde tuttuğunuzda gittiği URL'i gösterir. Eğer bağlantının gittiği yer beklenmedik veya yabancı ise, gönderenin gerçek olup olmadığını teyit edin. Bağlantılar her zaman "https://" ile başlamalıdır. Eğer "data://" ile başlıyorsa bu kesinlikle bunun bir oltalama saldırısı olduğuna işarettir.

Bilinmeyen kişilerden veya şüpheli görünen e-postalarla gelen bağlantıları ve dosyaları asla açmayın. Tanıdığınız kişilerin aksine bilinmeyen kimseler size gerçekten ihtiyacınız olacak bir bağlantı veya dosya göndermeyecektir. Eğer bilinmeyen bir gönderenin bağlantısı gerçekten gerekli bir bilgi içeriyorsa, bu bilgiye webte yapılacak bir arama gibi daha güvenilir bir yolla ulaşmak mümkündür.

Bir bağlantıya tıkladıktan sonra asla hesaplarınıza giriş yapmayın

Eğer e-posta ile gelen bir bağlantıya tıklarsanız, açılan sayfada herhangi bir hesabınızın bilgileri ile giriş yapmamanız önemlidir. Eğer bir web sayfası sizden giriş yapmanızı isterse şu adımları takip edin:

1. Tarayıcınızda yeni bir sekme açın ve alan adını elle tekrar girin.
2. Yeni açtığınız sekmeden hesabınıza giriş yapın.
3. E-postadaki bağlantıya geri dönüp tekrar tıklayarak açın.
4. Bağlantı açıldığında sizden giriş yapmanızı istemiyor olması gerekir. Eğer yine de giriş yapmanızı istiyorsa bu e-posta muhtemelen oltalama saldırısıdır.

Bu yöntem sizi çoğu oltalama saldırısından koruyacaktır.

Dosya eklerinden uzak durun

E-posta ekleri, oltalama saldırıları için aracı olmak dahil ciddi tehlikeler içerir. Dosya eklerinin gönderen ile alıcı arasında takip edilmediği veya değiştirilmediğine dair güvence yoktur. Haliyle gönderdiğiniz ekin alıcıya ulaşan ek ile aynı dosya olduğuna emin olamazsınız. Sizin ile alıcınız arasındaki kötücül bir sunucu, gönderinizi istediği gibi bir virüs veya kötücül yazılım ile değiştirebilir. Ek olarak gönderilen dosyalar alıcının, kontrol edilmesi kolay olmayan e-posta kutusunda kalmaktadır. Örneğin, kredi kartı bilgilerinizi içeren bir ödeme formunu satıcıya göndermeniz durumunda satıcı silmediği sürece o bilgi kendilerine ait e-posta sunucusunda duracaktır. Bir ihlal olması durumunda, sunucuya giren saldırganlar gönderdiğiniz bilgiye de erişecektir.

Dosyaları e-posta eki olarak göndermek yerine, bir sunucuda tutup bağlantılarını e-posta ile göndermek daha iyi bir çözümdür. İdeali, bu bağlantıların dosyaları bir parola ile koruduğu veya bir tür yetkilendirme sistemi ile giriş yapılan ve bir süre sonra süresi geçen sistemlerle sunulmasıdır. Bu bağlantılar, çoğu veri depolama sistemi tarafından kolaylıkla üretilebilmektedir. Kendi sunucunuzda duran veya uzak sunucularda bizzat çalıştırdığınız sistemler bu imkana sahip olabilir. (Örn. Nextcloud)

Geçici bir bağlantı ile dosya göndermek istiyorsanız, https://share.riseup.net servisini kullanabilirsiniz. Yararlanabileceğiniz ek kaynaklar için dipnot kısmına göz atın[1]

Parolalar

Parola yöneticisi kullanın

Parola yöneticisi kullanmak, kişisel güvenliğinizi arttırmak için yapabileceğiniz en önemli değişikliktir.

Bilgisayarların işlem güçlerinin giderek arttığı ve sızıntılar dolayısı ile çokça kişinin parolaları İnternet'e saçıldığı için insanların kafalarından uydurduğu parolalar artık yetersiz kalmaktadır. Güvenli parolalar artık *xoo|Z'eetohth3Zoaph^* gibi göründüğünden insanların hatırlaması mümkün değildir.

Bir parola yöneticisi, size hem güçlü hem de eşsiz parolalar kullanma imkanı sağlar. Parola yöneticisi ile her hesabınız için benzersiz parolalar atar ve tüm hesaplarınızın parolalarına erişmenizi sağlayacak sadece bir adet parola hatırlarsınız. Özetle siz bir tane güvenli parola hatırlarsınız, parola yöneticisi sizin için yüzlerce!

İyi bir parola yöneticisinde dikkat edilmesi gereken üç önemli özelliği vardır:

Yerel Uygulama: Parolalarınızı, bir ana parola ile şifreleyerek saklayan özel bir uygulamadır. Bu oldukça güvenilir bir seçenek olmakla birlikte birden fazla cihaz arasında eşitlemeyi güçleştirecektir.

Bulut Hizmetleri: Genellikle ücretli olmakla parolalarınızı cihazlarınızdan bağımsız olarak saklayan bir hizmeti ifade eder. Bulut hizmetleri aracılığı ile parolalarınıza her yerden ulaşmanın kolaylığı olmakla birlikte dezavantajı daha az güvenliğe sahip olmasıdır.

1. Security Self-defense / How to Avoid Phishing Attacks
2. Security Education Companion / Phishing and Malware
3. Security In-a-box / Protect Your Device From Malware and Hackers
4. Security In-a-box / Keep Your Online Communications Private
5. Security Planner / Spot Suspicious Emails

Tarayıcı Eklentileri: Hem yerel uygulama hem de bulut hizmeti olarak sunulan parola yöneticileri çoğunlukla, parolalarınıza kolaylıkla erişebilmeniz için bir tarayıcı eklentisine sahiptirler. Bu eklentiler rahatlık sağlar fakat daha az güvenlidirler.

Özgür Yazılım: Kullanacağınız parola yöneticisi muhakkak özgür bir yazılım olmalıdır. Nasıl çalıştığını bilemediğiniz bir yazılıma parolalarınızı teslim etmek güvenli değildir.

Hangi aracı seçtiğinize bakmaksızın gerçekten önemli olan bir parola yöneticisi kullanmanızdır. Lütfen aşağıdaki önerileri aklınızda tutun:

Ana Parola: Bir parola yöneticisi kullanırken, ana parolanızı kaybetmemeniz hayati önem taşır. Ana parolayı unutma ihtimaline karşı bir yere bu parolayı not edebilirsiniz. Ama güçlü ve unutulması zor bir ana parola üretmek için Zarola kullanmanızı öneriyoruz. Bilgisayarlar için zor ama hatırlamanız için kolay bir parola tüm sayısal hayatınızın dayanacağı bir parolayı unutmamak için en garanti yoldur.

Yedekler: Parola yöneticinizin verilerini düzenli olarak yedeklemeniz de bir o kadar önemlidir. Bulut hizmeti yedekleme işini sizin için yaparken yerel yedeklerinizi düzenli olarak almanız yararınıza olacaktır. Yerel uygulamalar için veri dosyasının yedeğini almak yeterlidir. Ara sıra parola yöneticinizin parolaları sakladığı küçük dosyayı bir USB belleğe koyup kenara kaldırmak sizi çokça baş ağrısından kurtarabilir. Güvenlik ile ilgilenenlerin sıkça söylediği şöyle bir söz vardır: "Verilerin 3 farklı yerde yedeklenmemişse, verilerin yoktur."

Yaygın özgür parola yöneticileri;

KeePassXC: (yerel uygulama) Kullanım kolaylığı açısından tavsiye edilen yerel parola yöneticisidir. Neredeyse her bilgisayarda çalışabilmektedir ve Nextcloud ile eşitlenebilir.

Pass: GnuPG ve Git ile çalışan bir parola yöneticisidir. Eğer GnuPG'ye ve Git'e biraz hakimseniz, kesinlikle pass kullanmanız tavsiye edilir. Pass, parolalarınızı GnuPG anahtarınızla şifreler ve uzak bir Git sunucusuyla eşitleyebilir. Android istemcisi ve Firefox eklentisi mevcuttur.

Bitwarden: Tamamen uzak sunucuda çalışan ve pek çok platform için istemcileri bulunan bir parola yöneticisidir.

Güçlü Parolalar Kullanın

Güçlü parolalar rastgele üretilirler. Bir parolanın gücünü, uzunluğu ve rastgeleliği belirler. Cihazınız ve parola yöneticisi ana parolası haricindeki tüm parolalarınız bir parola yöneticisi tarafından rastgele üretilmelidir. Parolalarınız en az 12 karakter olmalıdır. Ancak 26 karakterden uzun parola kullanmanıza gerek yoktur. İyi bir parola geleceğe yönelik iyi bir yatırımdır. İnsanlar, bilgisayarların aksine güvenli

parolalar yaratmakta bir hayli başarısızdır. Bırakın bilgisayar bu işi sizin için yapsın. Hatırlamanız gereken parolalar üretmek için pek çok yol bulunmaktadır. Eğer parola yöneticisi kullanıyorsanız bırakın uygulama sizin için üretsin. Ancak kendiniz hatırlaması kolay güçlü parolalar oluşturmak istiyorsanız bir Password Generator kullanmanızı öneriyoruz.

https://passwordsgenerator.net, kolayca hatırlanabilir ve yüksek derecede güvenli parolalar oluşturabilmenizi sağlayan bir yöntemdir. Ancak bu durumda aklınıza şöyle bir soru gelmiş olabilir: "Password Generator oluşturduğu şifreleri kaydediyor mu?"

Password Generator bu şifreleri kaydetse bile, nerede kullandığınızı bilmediği için sorun olmayacaktır. Ama yine de isterseniz C/C++/C# ya da Python gibi dillerle kendi Password Generator toolunuzu kodlayabilirsiniz. Nasıl yapacağınızı bilmiyorsanız ChatGPT'ye sorarak kolayca yapabilirsiniz.

Konuya ilişkin Security Self-defense'in "Güçlü Parolalar Üretmek" rehberine bakabilirsiniz.

Her hesabın güvenli ve eşsiz bir parola ile korunması önemlidir, çünkü bir hesaba erişim bazen diğer hesap ve sistemlere erişim hakkı doğurabilir. Bu durum, özellikle hesaplarınızı sıfırlama imkanı olan her e-posta hesabı için geçerlidir (genellikle "parolamı unuttum" bağlantıları ile).

Eşsiz parolalar kullanın

Eşsiz parolalar kullanmak üçüncü parti hizmetleri kullanırken alınan riskleri en aza indirir. Şayet bir parolayı birden fazla hesap için kullanırsanız, bir hesaptan sızan kullanıcı adı ve parolalar ile diğer hesaplarınıza sızılabilir. Farklı servisler için farklı parolalar kullanmak hesaplarınızı birbirinden izole ederek riski azaltacaktır. Bir parola yöneticisi kullanmak bunu yapmayı oldukça kolaylaştırır.

Parolalarınızı gizli tutun

Parolalarınızı her kim sorarsa sorsun asla kimseye vermeyin (Evet, teknik destek vermek için soran IT personeline de vermeyin.). Neredeyse her hesap ve sistem parola sıfırlamasına olanak tanımaktadır. Herhangi bir IT uzmanı, size parolanızı sormadan bakım amaçlı parolanızı sıfırlayabilmektedir. Bu tip sistemler aynı zamanda erişimleri takip altında tutar, sizi sıfırlama hakkında bilgilendirir ve her yönetici erişiminden sonra parolanızı değiştirmeniz istenir. Bunun için sadece söz konusu sistemlere erişiminizin olması yeterlidir.

Kurumsal ve kişisel parolalarınızı ayırın

Burada kurumsal paroladan kasıt, kurumunuzun sistemlerine ve dijital kimliklerine erişim sağlayan herhangi bir paroladır. Bunlar gerçekten önemli bilgiler olduklarından, kişilerin kendi kişisel hesaplarına girmek için kullandıkları

parolalardan farklı olmalı ve ayrı olarak saklanmalıdır. Kurumsal parolanızı, parola yöneticisinde ayrı bir giriş veya farklı bir parola dosyası kullanarak, ya da tamamen farklı bir parola yöneticisi seçerek saklayabilirsiniz.

Konuyla alakalı yararlanabileceğiniz ek kaynaklar:

- Security Planner / Password Managers
- Security In-a-box / Passwords
- Security Self-defense / Animated Overview: Using Password Managers to Stay Safe Online
- Security Self-defense / How to: Use KeepPassXC
- Security Self-defense / Creating Strong Passwords
- Security Education Companion / Passwords
- Security Education Companion / Password Managers

Çift aşamalı doğrulama kullanın

Çift aşamalı doğrulama veya kısa adı ile 2FA (Two Factor Authentication) bir sisteme veya hesaba erişim için iki farklı girdinin gerekmesi demektir. Genellikle girdilerin kaynaklarının veya elde edilme şekillerinin farklı olması istenir. Sadece parola ile giriş yapılan sistemlerde "parola" bilinen bir şey olarak bir aşamayı ifade eder. Bunun yanında bir başka "şey" daha gerekmesi durumunda ikinci aşama elde edilmiş olur.

Bugün bankacılık işlemleri yapan neredeyse herkes 2FA'nın en yaygın metoduna aşinadır. Bankacılık sistemine giriş yaptığınızda banka sizden parolanızı girmenizi istediği gibi bir de atılan SMS'teki kodu girmenizi ister. Bu durumda parolanız bildiğiniz bir şey olarak ilk aşamayı, SMS'in gönderildiği SIM kart da sahip olduğunuz ikinci aşamayı oluşturur. Bu bakımdan bir kişinin hesabınıza erişmek için hem parolanızı öğrenmesi hem de SIM kartınız ile birlikte onun parolasını da bilmesi gereklidir.

2FA nasıl kullanılır?

2FA kullanımı hesaplarınızın hizmet sağlayıcısına bağlıdır.

- SMS aracılığıyla: Pek çok hizmet size SMS ile bu imkanı sunacaktır. SMS uygulaması kolay bir yol olduğundan tercih edilmektedir. Fakat GSM şebekesi doğası gereği güvensiz olduğundan size gönderilen kodun çalınması veya SIM kartınızın çeşitli şekillerde kopyalanması sizi riske atabilir. Aynı zamanda kişisel veriniz ve günümüzde kimliğinizin bir parçası olan cep telefonu numaranızı vermek anonimliğinizi bozacağı gibi güvenliğinizi tehlikeye de atabilir.

- Yazılım aracılığıyla: Akıllı cihazlarınıza kurabileceğiniz bir yazılım aracılığıyla 2FA kullanmanız mümkün olabilir. Bu imkan her zaman SMS'e tercih

edilmelidir. Cihazınız zamana bağlı olarak çoğunlukla 60 saniye geçerli kodları yerel olarak üretecek ve size gösterecektir. Bunu yapmak için ilgili yazılımı çalıştırmanız ve hesap yöneticisinin size gösterdiği adımları takip edip ilgili karekodu okutmanız yeterlidir.

FreeOTP+ ve andOTP, Android cihazlarınızda 2FA kodları üretmek için kullanabileceğiniz özgür yazılımlardır.
andOTP kullanım rehberi

- Donanımsal anahtarlar ile: Özellikle çift aşamalı yetkilendirme için tasarlanmış cihazlar güvenlik için en iyi çözümdür. Lakin donanımların pahalı olması sebebi ile pek az hizmet bu yöntemi tercih etmektedir. Bu amaçla kendi cihazınızı alıp yazılım yerine bu cihazlar ile kod üretimi yapabilirsiniz.

Yubikey: Sadece bir 2FA cihazı olmaktan çok daha fazlasını yapabilen en yaygın kullanılan çift aşamalı yetkilendirme cihazıdır. Birden fazla protokolü desteklemekle tavsiye edilebilecek ilk üründür.

RSA Tokens: Bulabilir ve kullanabilirseniz RSA donanımlarını kod tabanlı 2FA uygulamalarında kullanabilirsiniz.

Yubikey 2FA Rehberi için bu sayfaya göz atabilirsiniz.

2FA kullanırken nelere dikkat edilmeli?

2FA başkalarının hesabınıza girmesini etkili şekilde engellediği gibi sizin de hesabınıza erişmenizi aynı şekilde engelleyebilir. Bu sebeple 2FA kodlarınızın gönderildiği SIM kartınızı veya kodların üretildiği cihazınızı korumalısınız. Hayat sürprizlerle dolu olduğundan genellikle SMS harici her 2FA uygulaması size çoğunlukla 10 tane yedek kod verir. Bu yedek kodları bastırarak güvenilir bir yerde saklamanız hatta bir iki tanesini cüzdanınızda taşımanız şiddetle önerilir. Bu şekilde ikinci aşamanızı kaybetmeniz durumunuzda hesaplarınızdan mahrum kalmazsınız.

Konuyla ilgili yardımcı olabilecek kaynak:

- Olağan Paranoya / Çift Aşamalı Kimlik Doğrulama İle Hesabınızın Güvenliğini Arttırın

Yazılımlarınızı Güncel Tutun

Bir saldırgan, yazılımlarınızdaki bir zayıflığı kullanarak cihazlarınızın güvenliğini tehlikeye atabilir. Bu riski yazılımlarınızı güncel tutarak önleyebilirsiniz. Yazılım geliştiricileri genellikle bu açıkları düzelterek güncellemeler sunar.

Özellikle işletim sisteminizi güncel tutmak önemlidir, çünkü işletim sistemi cihazınızdaki her işleme ayrıcalıklı erişim sağlar.

Otomatik Güncellemeler Nasıl Açılır?

- GNU/Linux: Çoğu dağıtımda otomatik güncellemeler açık gelir.
    - Debian, Ubuntu: `sudo apt-get update && sudo apt-get upgrade -y`
    - Red Hat, Fedora: `sudo yum update -y`
    - Arch, Manjaro: `sudo pacman -Syu`

- macOS: Apple menüsüne tıklayın, Sistem Tercihleri > App Store > Güncellemeleri Otomatik Olarak Denetle.

- Windows: Başlat çubuğuna tıklayın, Ayarlar > Güncelleme ve Güvenlik > Windows Güncellemeleri > İleri Seçenekler > Otomatik (önerilen).

Uygulama mağazasını kullanın

Mümkün olduğunca yazılımlarınızı işletim sisteminize ait uygulama mağazasından indirmelisiniz;

- **Güvenilirdir:** Uygulama mağazasındaki uygulamalar geliştiricileri tarafından imzalanır ve mağaza tarafından doğrulanır. Bu doğrulama çoğu zaman sığ bir inceleme olduğu için mutlak olarak güven duyulmamalıdır ama hiç yoktan iyidir.

- **Güncellemeler için efektiftir:** Uygulama mağazası uygulamalarınızı güncel tutmanıza yardım eder.

- **Side Loading Saldırılarını Önler:** Uygulama mağazası dışından uygulama indirmeye "side Loading" denir. Side loading şu anda Android'de varsayılan olarak engelli, iOS'te ise imkansız ancak GNU/Linux'ta ve macOS'te seçime bağlı durumdadır. Windows sistemler ise çoğunlukla side loading'e dayanmaktadır. Side loading kullanarak indirdiğiniz ve doğrulamadığınız her yazılım nihayetinde sisteminizi kötücül yazılımlara karşı tehlikeye atar. Bu neden ile sistemlerinize kurduğunuz yazılımları güvenilir kaynaklardan ve uygulama mağazalarından yüklemeniz önerilir.

Not: Resmi Android uygulama mağazası Google Play'i taklitçi uygulamalardan kaçınmak için dikkatli kullanmalısınız. En iyisi sadece özgür yazılımların sunulduğu **F-Droid** uygulama mağazasını kullanmanızdır.
GNU/Linux sistemlerinde ise işletim sisteminize ait olmayan ama güvenilir olan bazı mağazalar vardır. Örn: Flatpak, Snap vs. Fakat bunlar zaten genelde sistemle yüklü gelirler.

Şüpheliyse indirmeyin

Mobil uygulamalar, tarayıcı eklentileri ve ücretsiz programların artması ile birçok güvenlik problemi de ortaya çıktı. Bu sebep ile güvendiğiniz kuruluşların (örneğin daha önce kullanmış olduğunuz) yazılım geliştiricileri tarafından geliştirilmeyen yazılımlardan mümkün ise kaçının.

Görünürde iyi niyetli olan veya faydalı görünen yazılımlar (virüs tarayıcıları gibi) aslında arka plandaki kötü hareketlerini gizliyor olabilir. Çoğu tarayıcıda ve mobil cihazda bir uygulama kurulum sırasında cihazda ulaşabileceği bilgiler ve donanımlar hakkında çeşitli izinler ister. Bu izinlerin uygulamanın beklenen amacı kapsamında kaldığına kabaca göz atmak gereklidir.Örneğin bir fener uygulaması cihazınızın rehberine erişmek veya telefon aramaları yapabilmek isterse bu yazılımı kullanmamalısınız. Aramalarınıza, kişilerinize, kameranıza, mikrofonunuza, konum servislerinize veya tüm saklama alanınıza verdiğiniz erişim izinleri hakkında çok dikkatli olunmalıdır.

İndirdikten sonra verdiğiniz izinlere bakmak, cihaza ve koşula göre farklılık gösterebilir. Firefox tarayıcısında, ayarlar altında "Mahremiyet ve güvenlik" sekmesinde verilen izinleri görebilirsiniz. Chrome ve Chromium'da, chrome://extensions/'a gidin ve her eklenti için izinlere tıklayın. iOS cihazlarında, ayarların altında tüm izinlerin listesi vardır. Her iznin altında da o izinleri kullanan uygulamalar yer alır. Android cihazlarında Ayarlar > Uygulama yöneticisinde uygulama listesini görüntüleyebilirsiniz. Her uygulamanın altında uygulamanın kullandığı izinleri gösteren bir liste vardır.

Genel bir alışkanlık olarak cihazlarınızda gereksiz veya çok seyrek kullandığınız yazılımları bulundurmamak gerekir. Şayet bir yazılımın sunduğu hizmeti Web'den alabiliyorsanız, yazılımını cihazınıza kurmak yerine tarayıcınız aracılığı ile web üzerinden hizmet almayı seçebilirsiniz. Genel olarak da bir yazılım hem özgür değil hem de ücret istemeden çok şey vaat ediyorsa işin içinde bir bit yeniği var mı bakılmalıdır.

Maalesef dizüstü ve masaüstü bilgisayarlarındaki çoğu işletim sisteminin bir izin yönetimi yok ve yazılımlar kurulum sırasında sistem kaynaklarına erişim için izin istemiyor. Bu yüzden bilgisayarlarınıza indirdiğiniz yazılımlarda çok daha dikkatli olmanız gerekiyor.

Korsan yazılım kullanmayın / Mümkünse mülk yazılım kullanmayın

Korsan yazılım indirmek bilgisayarınıza virüs veya kötü amaçlı yazılım bulaştırmak için harika bir yoldur. Pek çok mülk yazılım da kaynak koduna erişemediğiniz için şüpheli ve bazen amacı gereği zaten güvenlik tehlikesidir.

Eğer cihazlarınızda yapmanız gereken bir işlem varsa ve bunun için uygun bir yazılım arıyorsanız öncelikle özgür yazılımları değerlendirmeniz önerilir.

Mülk yazılım yerine Özgür yazılım kullanın

Özgür yazılımlar, genellikle kullanılan özel mülk yazılımlara harika alternatiflerdir. GNU/Linux, Windows, macOS ve Android için kolaylıkla elde edilebilir.

- **Mozilla Firefox**: Web tarayıcısı (Google Chrome alternatifi)
- **Mozilla Thunderbird**: E-posta istemcisi (Microsoft Outlook alternatifi)
- **VLC media player**: Medya oynatıcı (Windows Media Player alternatifi)
- **GIMP**: Taramalı grafik ve fotoğraf düzenleme programı (Adobe Photoshop alternatifi)
- **Krita**: Bit eşlem grafik ve fotoğraf düzenleme programı (Adobe Photoshop alternatifi)
- **Inkscape**: Vektör çizim programı (Adobe Illustrator alternatifi)
- **LibreOffice**: Ofis yazılımı (Microsoft Office alternatifi)
- **Scribus**: Masaüstü yayıncılık uygulaması (Adobe InDesign alternatifi)
- **F-Droid**: Android işletim sistemlerinde özgür yazılımların bulunabileceği benzersiz bir uygulama deposu. (Google Play Store alternatifi)
- **Signal**: Mesajlaşma uygulaması (Whatsapp alternarifi)
- **Ollama**: Lokal olarak çalışan, özgür yazılım olan AI (ChatGPT alternatifi)

Herhangi bir uygulamanın açık kaynak alternatifini bulmak istiyorsanız, AlternativeTo sitesinde o uygulamayı aratıp, “Open Source” ve “Free” filtrelerini seçebilirsiniz.

Cihazlarınızı neden şifrelemelisiniz?

Cihazlarınızı şifrelemekle, cihazınızın depolama alanındaki; işletim sisteminizi, kurduğunuz yazılımları ve kişisel verilerinizi içeren bölümleri cihazınız kapalıyken parolasını bilmeyenlere karşı erişilmez kılarsınız.

Cihazınız şifreli değil iken çalınması kaybolması durumunda cihazınızı bulan herhangi biri kolaylıkla dosyalarınızı okuyabilir, hesaplarınıza erişebilir ve kimliğinizi çalabilir. Daha kötüsü, bir saldırgan kötücül yazılımları cihazınıza yükleyerek tüm kullanımınıza uzaktan erişebilir.

Cihazlar nasıl şifrelenir?

Tam disk şifreleme (Full disk encryption) bazı mobil cihazlarda olağan olarak gelmekte olsa da dizüstü ile masaüstü bilgisayarlarda ve çoğu cep telefonunda elle ayarlanmalıdır.

Bilgisayar Kurulumları:

- **GNU/Linux:** Neredeyse her GNU/Linux dağıtımı kurulumu sırasında diskinizi şifrelemeyi mümkün kılar. Bu amaçla iki yöntem söz konusudur:
  - **"Tam Disk" Şifreleme:** GNU/Linux dağıtımlarında **LUKS** artık standart olarak desteklenmektedir. Bu yöntem cihazınızın ana depolama

alanındaki işletim sistemi dahil her şeyi şifreler. Cihazınız açılırken size ayrı ve deşifre amacıyla bir parola sorulur.

  - **"Ev Dizini" Şifreleme:** Bu yaklaşımda ise işletim sistemi şifrelenmez. Kişisel verileriniz korunacaktır fakat bir saldırganın cihazınıza eriştiğinde işletim sisteminize etki edecek bir değişiklik yapmasını engellemeyecektir.

- **Windows:** Security Planner / Windows Şifrelemesi
  - Önemli: Microsoft, standart olarak şifreleme anahtarlarınızı uzak sunucularda yedeklemektedir. Bu Microsoft'un ve iş birliği yaptığı her devletin cihazınızı kolaylıkla deşifre edebilmesi demektir. Eğer bir devletin cihazınızın içeriğine erişmesinden endişeli iseniz bu "özelliği" devre dışı bırakmalısınız ve yeni anahtarlar üretmelisiniz.
- **macOS:** Security Planner / Mac Şifreleme

Cep Telefonu Kurumları:

- **iOS**: Security Planner / Apple iOS Şifreleme
- **Android:** How to Encrypt Your Android Phone (and Why You Might Want to) / Android Cihaz Şifreleme
- **Android:** Full-Disk Encryption / Android Cihaz Şifreleme
  - Önemli: Cihazınızı şifrelemeden önce cihazın şarjının en az %80 ve şarja bağlı olmasına dikkat ediniz. Öncesinde yedeklerinizi alınız. İki kaynağı da inceleyebilirsiniz ancak How to Encrypt Your Android Phone (and Why You Might Want to) kaynağına pratik çözüm olarak bakabilirsiniz.

Cihaz şifrelemenin zorlukları

Sınırları: Cihaz şifreleme her derde deva değildir! Eğer parolalarınız yeterince güçlü değil ise bir bilgisayar rahatlıkla parolanızı tahmin edebilir ve cihazınıza erişilebilir. Ayrıca cihaz şifreleme virüslere ve kötücül yazılımlara karşı hiçbir koruma sağlamaz. Eğer verileriniz bir bulut hizmetine yedeklendiyse ve bu hizmeti sağlayan sunucular açığa çıkar veya devletle iş birliği yaparsalarsa cihaz şifrelemesi verilerinizi korumayacaktır (kullanılan hizmet özellikle uçtan uca şifreleme desteklemiyorsa).

Yetkilendirme etkinleştirilmelidir

Cihaz şifrelemesi, yetkilendirme zorunlu değilse etkili değildir. Örneğin dizüstünü bilgisayarınıza giriş yapmanız veya cep telefonunuzun ekran kilidini bir PIN ile korumanız gibi...

Veri kurtarmayı imkansız kılar

Tam disk şifreleme, iyi bir parola ve PIN yönetimi sürdürülmüyorsa verilerinize erişiminizi kaybetme riskinizi arttırır. Unutulan bir parola veya PIN, disk şifreleme anahtarının bulunduğu sektörde yaşanan bir arıza verilerinizi sizin veya bir başkasının kurtaramayacağının garantisidir. Verilerinizin düzenli yedeklerini alarak veri kaybı riskini azaltmalısınız. Yedeklerinizi de fiziki güvneliğini sağlayamıyorsanız şifrelemeniz önerilir.

Cihaz kapalı veya kilitli olmalıdır

Cihaz şifrelemesi sadece bilgisayarınız kapalı iken tam güvenlik sağlar. Bir kere parolanız ile giriş yaptıktan sonra bilgisayarınız, verilerinizin deşifre edilmesi için gerekli anahtarı hafızasına almış olmakla ekran kilidi etkin olsa bile çalışır durumda olduğundan (veya uyurken) bir kişinin verilerinize erişme riskini taşır. Bu tip bir saldırı fazlasıyla teknik yetkinlik gerektirmekte ve bu risk bilgisayarınızı açık tutmanıza veya giriş yapmanıza engel olmamalı. Fakat cihazınızın sizden uzak kalabileceği tehlikeli durumlarda bilgisayarınızı kapalı tutmak en iyisidir. Eğer bu tip bir saldırının kurbanı olmaktan endişeli iseniz en iyisi cihazınızı fiziksel olarak her zaman yanınızda bulundurmalısınız.

Konu hakkında daha fazla bilgi için önerdiğim kaynaklar:

- Security In-a-box / Güvenli Dosya Depolama
- Security Planner / Windows Şireleme
- Security Planner / Mac Şifreleme
- Security Planner / Apple iOS Şifreleme
- How to Encrypt Your Android Phone (and Why You Might Want to) / Android Cihaz Şifreleme
- Full-Disk Encryption / Android Cihaz Şifreleme
- Security Self-defense / iPhone'nunuzu nasıl Şifrelersiniz

Optik Diskler

Optik disklerin güvenlik kullanımları

Optik diskler çoğu kayıt ortamı gibi fiziki ve sayısal kimi özellikler içermektedir. Bu özellikler günümüzün elektriksel kayıt sistemlerinden farklılıklar göstermekle özel durumlarda tercih edilebilir olmaktadır.

- Optik diskler hafif ve incedir.
- Optik diskler elektronik bir aksam içermediğinden çevresel ve mekanik etkilere dayanıklıdır.
- Elektronik veya metal aksam içermediğinden x-ray veya manyetik dedektör gibi araçlarda daha az görünürlerdir.
- Optik diskler gözden çıkarılabilecek kadar ucuzdur.
- Optik diskler tekrar yazılabilir versiyonları hariç bir kere yazıldıktan sonra değiştirilemezler.

Yukarıda sayılan özelliklerden taşınan verinin güvenlik gereksinimlerine veya taşımanın gerektirdiği güvenlik koşullarına göre faydalanılabilir.

Optik disklerin saklama kullanımı

Optik disklerin mekanik parçalar içermemesi ve dış etmenlere olan dayanıklılığı çeşitli verilerin güvenli şekilde saklanması için değerli bir özellik oluşturmakta. Her ne kadar büyük kapasiteler sunmasa da önemli verilerin yedeklerinin oluşturulması ve bu yedeklerin güvenli konumlarda saklanmasına imkan sağlamaktadır. Bu bakımdan aşağıdaki örnek koşullarda optik diskler tecih konusu olabilir:

- Kriptografik anahtar ve araçların yedeklerinin saklanması
- Offline tutulması gereken hassas verilerin yedeklenmesi ve saklanması
- Optik disklerin taşıma kullanımı
- Optik disklerin en değerli kullanımlarından biri veri taşıma ihtiyacında ortaya çıkmaktadır. Optik disklerin ucuz olmaları ve ince yapıları sebebi ile gözden çıkarılabilir şekilde çeşitli aracılar veya riskli alanlardan taşınması mümkün olmaktadır.

- Posta yolu ile anonim şekilde gönderilmeleri

- Sınır güvenliği gibi riskli alanlardan fark ettirilmeden geçirilebilmeleri
- El koyulması durumunda ekonomik bir endişeye yol açmaması

Optik disklerin teknik faydaları

Veri güvenliğinin operasyonel koşullarında bir verinin optik disk üzerinde tutulması veya işlenmesinin olası faydaları bulunmaktadır.

- Optik diskler çok hızlı şekilde imha edilebilirler.
- Optik diskler bir kere yazıldıktan sonra değiştirilemedikleri için üzerindeki verilerin bütünlüğünü korurlar.
- Optik diskler kolayca depolanabilir ve fazla yer kaplamazlar. Hareketli parça içermediklerinden mekanik olarak görece dayanıklı sayılırlar.

Şifreli optik disk oluşturmak

Bir optik diskteki verileri şifrelemenin pek çok yolu bulunmakta. GPG kullanarak tüm dosyaları şifreleyip diske yazmak mümkün olduğu gibi uzak sunucudaki dosyaların şifrelendiği şekilde şifrelenen dizini olduğu gibi diske yazdımak da mümkün.

Bu rehber LUKS ile bir optik diskin şifrelenmesini anlatacaktır. Bu yöntemin yukarıdaki seçeneklere göre birkaç faydası bulunmakta.

- Tüm **GNU/Linux** sistemler Luks aygıtları otomatik olarak açabilmekte ve dosya sistemini gösterebilmekte. Bu sebepten diskin kullanımı çok kolaylaşmakta.
- Crypfs ve GPG gibi ayrı bir yazılımın kullanımına gerek kalmadan deşifre işlemi yapılabilmekte.
- Dosya dizinleri ve boyutları gibi üstverilerin ifşası engellenebilmekte.

Bu rehberi takip edebilmek için bir herhangi bir GNU/Linux dağıtımını kullanmanız, root erişimine ve bir disk yazıcıya sahip olmanız gerekmekte. Rehber DVD kapasitesini esas almakla birlikte boyutları dilediğiniz şekilde değiştirmeniz mümkündür.

Boş bir dosya yaratın

İçine verilerin yazılacağı boş bir dosyaya ihtiyaç duyulmakta. Bunu basitçe /dev/zero ile sıfır yazarak yaratabilecek olsak da şifreli verinin diskteki boşluk

alanlardan ayırt edilememesi için aşağıdaki şekilde rastgele verilerden bir dosya oluşturun.

```
dd if=/dev/urandom of=disk.img bs=1M count=4400
```

Count değerini kullandığınız medyanın boyutuna göre ayarlayabilirsiniz. Yukarıdaki komut 4.4Gb boyutunda disk.img adlı bir dosya oluşturacaktır.

Luks dosyasını oluşturup dosyalarınızı ekleyin

Aşağıdaki komut sırası ile Luks imajını oluşturup dosyalarınızı yedekleyebilirsiniz. Dosyalarınızın konumunu ile belirtlen yere koymayı ihmal etmeyin.

```
sudo losetup /dev/loop1 disk.img && cryptsetup luksFormat /dev/loop1 &&
cryptsetup luksOpen /dev/loop1 yedekdisk && genisoimage -R -J -joliet-long -
graft-points -V backup -o /dev/mapper/yedekdisk <yedeklenecek dizinin yolu>
```

Yukarıdaki çeşitli komutlar sıra ile çalışacak ve size sıra ile kullanmak istediğiniz parolayı iki kere soracak ve ardından gösterdiğiniz dizindeki dosyaları oluşturulan dosyaya şifreli olarak aktaracaktır.

Luks dosyasını kapatın

Dosyanın oluşturulması tamamlandıktan sonra aşağıdaki komut ile bilgisayarınızda bağlı bulunan aygıtları kaldırarak imaj dosyasının işleminin tamamlayın.

```
sudo cryptsetup luksClose /dev/mapper/yedekdisk && losetup -d /dev/loop1
```

disk.img dosyasını yazın

Tercihiniz olan bir yazdırma yazılımı ile disk.img dosyasını diskinize yazabilirsiniz. Yazma işleminin bitmesinin ardından diskinizi cihazınıza taktığınızda şayet otomatik başlatma ayarlı ise diskinizin parolası sorulacak ve doğru girmeniz durumunda dosya yöneticinizde disk içeriğini şifresiz olarak görebileceksiniz.

Yönlendirici Güvenliği

Evinizin köşesinde unuttuğunuz, telefon kablosuna bağlı ve sadece İnternet bağlantınız kesildiğinde hatırladığınız küçük siyah kutular güvenliğiniz için önemli bir rol üstlenmektedirler. Bu cihazlar sizi internet servis sağlayıcınıza, cihazlarınızı da bir yerel ağ altında birbirine bağlar.

Modem ile yönlendirici teknik olarak farklı şeylerdir. Modem (modulator demodulator kelimelerinin birleşimi) iki nokta arasında bağlantı kurularak veri aktarılmasını sağlayan bir cihazdır. Bir zamanların çevirmeli bağlantı için kullanılan 56k modemleri gibi ADSL ve VDSL teknolojileri de sizi internet servis sağlayıcınıza bağlar. Dünya'da kullanımı artık yok olmakta olsa da Türkiye hala fiberoptik altyapı eksikliği altında bu teknolojileri yaygın olarak kullanmaya devam etmektedir.

Yönlendirici (router) bir ağı alt ağlara bölmeye yarayan ve aralarındaki trafiği düzenleyen bir donanımdır. Özel olarak tasarlanmış minik bir bilgisayar olmakla birlikte cihazlarınıza kablosuz bağlantı sağlamak ve denetlemekle görevlidir.

Modem olarak satılan cihazlar aslında bir modem ve yönlendiricinin birleşiminden oluşur. Bu bakımdan modeminizin arkasına bir yönlendirici daha eklemenize engel olan bir şey olmadığı gibi modemi ayrı bir donanım olarak alıp bir yönlendiriciye bağlamanız da mümkündür.

Yönlendiricilerin İnternet bağlantınızda ve yerel ağınıza (cihazlarınızın birbirini görebildiği iç ağınız) hakim olması onları güvenliğinizin önemli bir parçası haline getirmekte. Yönlendiricinizin kontrolünde olan bir kişi aşağıdaki saldırılarla sınırlı olmamakla pek çok saldırıyı gerçekleştirebilir:

- Yerel ağınıza bağlı olan cihazları takip edebilir kaydedebilir.
- İnternet bağlantınızın gittiği yerleri ve şifresiz iletişimleri takip edebilir.
- Sizi güvenliğinizi tehdit edecek şekilde sahte sitelere yönlendirebilir.
- Ağınızdaki diğer cihazlara ulaşıp onların güvenliğini aşabilir.
- Ağınızda bulunan depolama aygıtlarına erişebilir ve dosyalarınızı çalabilir.

Bu tehditler ve bunun gerçekleşme ihtimali düşük olasılıklar içermez. Dünya'da pek çok kere yönlendiriciler yüzünden risk altına girmiş kullanıcılar oldu. Bunun sebepleri arasında; yönlendirici üreticisinin kötü güvenlik uygulamaları, internet servis sağlayıcılarının dağıttığı yönlendiricilere güvensiz ve onaysız uzaktan erişim

portları açması, güncellenmeyen veya güncellemesi artık olmayan cihazlardaki güvenlik açıkları sayılabilir.

Bu kadar önemli bir cihazın görece önemsiz görüntüsü nedeni ile ihmal ile karşılanması görece doğal karşılanabilir fakat çok basit tedbir ve değişikliklerle söz konusu cihazların güvenliği sağlanabilir.

Yönlendirici ve modem arayüz parolanızı değiştirin

Ağınızda bulunan her cihaz yönlendiricinizin ayarlarının yapıldığı arayüze bir web tarayıcısı aracılığı ile erişebilir. Bu durumda cihazınızın ayarlarının değiştirilmesi gibi istenmeyen sonuçlar ortaya çıkabilir. Pek çok yönlendirici standart "admin/admin" gibi parolalarla geldiklerinden bu ayarın kullanımın ilk anında değiştirilmesi gereklidir.

Yönlendiricilerde farklı olabilmekle birlikte çoğu yönlendirici *192.168.1.1* adresinden erişilebilir. Cihazınızdaki web tarayıcısına adresi girdiğinizde karşınıza giriş sayfası çıkacaktır. Buradan cihazınıza ait standart parola ile giriş yaptıktan sonra ayarlar içinden bu parolayı değiştirebilirsiniz.

Wifi parolalarınızı güvenli kılın

Wifi güvenliği neredeyse her köşede verilen bir tavsiye fakat pek çok insan için pratik gereklilikler altında ihmale uğramakta. Wifi ev ağınızı radyo dalgaları ile belki de yüzlerce metre uzaklara ulaştırmakta ve hiç göremediğiniz biri tarafından erişilebilmesine imkan verebilmekte.

Belki pek çok insan wifi güvenliğinin gerekliliğinin farkında ama misafirlerine güvenli bir parolayı aktarmanın zorluğuna katlanmamak için cep telefonu numaralarından "12345678" gibi bariz girdileri parola olarak kullanmakta.

Bu neden ile wifi parolalarınızı rastgele 16-24 karakter uzunluğunda bir değer ile değiştirmeniz tavsiye edilir.

Kablosuz ağınızın kullandığı şifreleme algoritmasının da günümüz gerekliliklerine uygun olduğunu denetleyin. WEP artık güvenli sayılmayan ve aşılması çok kolay bir güvenlik tedbiri olarak kesinlikle tavsiye edilmemektedir. Bunun yerine modern WPA2 şifrelemeyi kullanmanız güvenli bir wifi ağı için gereklidir.

Ağınıza güvendiğiniz misafirler olsa bile bilinmeyen cihazları eklemeniz önerilmez. Bu bakımdan kimi yönlendiriciler yalıtılmış ve sadece İnternet bağlantısı sağlayan "misafir" ağları oluşturabilir. Cihazınız bu imkanı sağlıyor ise kullanmanız kesinlikle tavsiye edilir. Şayet parolanızı misafirlerinizle kolaylıkla paylaşmak isterseniz karekod yardımı ile cihazların kolayca tarayıp bağlantı sağlayabileceği karekodlar oluşturabilirsiniz.

Mümkün ise wifi kullanmayın

Wifi çok rahat bir kullanım sağlasa bile her halukarda cihazınızı erişiminiz olmayan dış dünyaya açarak bir saldırı imkanı doğurur. Tüm yazılımlar ve donanımlar gibi bilinmeyen güvenlik açıklarının var olduğu bir dünyada bu kimi zaman kabul edilemeyecek bir risk taşıyabilir.

Kablolu bağlantılar hem daha istikrarlı bağlantı sağlar hem de ağınız ile ilgili bilgilerin dışarıya radyo dalgaları ile sızmasını engeller. Bu neden ile şayet wifi ağına ihtiyacınız özellikle yok ise cihazlarınızı kablo ile bağlayıp wifi ağınızı tamamen kapatmanız faydalı olabilir. Bu aynı zamanda Google gibi mahremiyet düşmanı şirketlerin ağınızın konumunu kullanıp kaydetmesine de engel olacaktır.

Not: Sıradan kullanıcı için Wifi kullanmak büyük bir sorun teşkil etmeyecektir. Eğer diğer güvenlik önlemlerini aldıysanız, Wifi kullansanız dahi büyük bir güvenlik açığınız olmayacaktır.

Cihazlarınıza fiziki erişimi sınırlandırın

Tüm güvenliği kritik cihazlarınız gibi yönlendiricinizin de ortalık yerde durması uygun bir durum sayılmaz. Bu bakımdan cihazınızı gözden uzak mümkünse erişimi kolay olmayan bir alanda saklamanız önerilir. Bu cihazınıza doğrudan erişimi engelleyerek çeşitli müdahaleleri görece zor kılacağından güvenliğinize katkı sunacaktır.

Cihazınızı güncelleyin

Pek çok yönlendirici satın alındıkları tarihten itibaren üreticisi tarafından belirli süreler ile güncellemeler ile desteklenmektedir. Ne yazık ki görece ucuz ve önemsenmeyen ürünler olmakla hem üreticiler tarafından gerekli güvenlik

güncellemeleri bir süre yapılmamakta ve kullanıcılar da gerekli güncellemeleri zamanında uygulamamakta. Bu tip açıklardan dolayı pek çok güvenlik açığı kablosuz bağlantı veya uzak erişim ile kullanıcılarının güvenliğini tehdit edebilmektedir.

Cihazınızın yönetim paneline girerek güncelleme seçeneklerine bakabilir veya üreticinin web sayfasından elinizdeki modelin sunulan en güncel yazılımına bakabilirsiniz. Şayet üreticiniz artık cihazınıza destek vermiyor ise özgür bir yazılım ile cihazınızı güncelleyebilir veya yeni bir modele geçerek destek alabilirsiniz.

Cihazınızı özgürleştirin

Her ne kadar yukarıdaki tavsiyeler genel olarak tüm yönlendiriciler için geçerli olsalar da üreticilerin pek de özen göstermedikleri ürünler olmakla son kullanıcı yönlendiricileri pek çok mülk yazılım içermekte ve potansiyel olarak incelenememiş güvenlik açıkları içerme ihtimali taşımakta. Bu duruma en iyi çözüm ise yazılım özgürlüğünden geçmekte. LibreCMC ve OpenWRT sayılması gereken en önemli projeler olmakla belirli donanımları güncel özgür sistemlerle güncelleyerek güvenliğinizi hatrısayılır miktarda arttırabilir ve cihazlarınızın kabiliyetini de geliştirebilirsiniz.

Özgür yönlendirici rehberi

Konudan bağımsız bazı önerilerim:

1. Bluetooth kullanmayın! (Nedeni: 1, 2, 3, 4, 5, 6, 7)
2. Açık alanlardaki bedava Wi-fi ağlarına bağlanmayın! (Nedeni: 1, 2, 3, 4, Onun yerine mobil ağ kullanmanız daha güvenlidir.)
3. VPN'lerin gizlilik sözleşmelerini okumadan onları kullanmayın! (Nedeni bu videoda gayet iyi anlatılmış sanırım: Popüler VPN'leri inceledim!)
4. iOS'a dikkat!
    1. Muhtemelen bir çoğunuz IOS'un Android'den daha az bilgi aldığını ve Android'den daha mahremiyet dostu olduğunu sanıyorsunuz. Bunun nedeni Apple sitesine girdiğinizde karşınıza çıkan "onu almıyoruz", "buna önem veriyoruz" gibi reklam amaçlı yanıltıcı yazılardır. Fakat durum düşündüğünüz gibi değil! Apple'nin sitesinden kolay kolay ulaşamadığınız gerçek gizlilik sözleşmesi var.

1. Bağlantılar:
    1. https://www.apple.com/legal/privacy/en-ww/
    2. https://www.apple.com/legal/privacy/data/en/apple-news/
    3. https://www.apple.com/legal/privacy/data/en/apple-music/
    4. https://developer.apple.com/app-store/app-privacy-details/
    5. https://www.apple.com/legal/privacy/data/en/app-store/
    6. https://www.apple.com/legal/privacy/data/en/apple-tv-app/
    7. https://www.apple.com/legal/privacy/data/en/apple-advertising/
    8. https://www.apple.com/legal/privacy/data/en/ask-siri-dictation/
    9. https://www.apple.com/legal/privacy/data/en/apple-id/
    10. https://edition.cnn.com/2019/08/28/tech/apple-siri-apology/index.html
2. Konuyla ilgili video: iPhonunuz Gizli Değil – Apple Verilerinizi Nasıl Kullanıyor?

5. "Linux'da virüs yok!" gibi yalanlara kanıp terminalinize bilmediğiniz komutları girmeyin.
    1. Linux'da gayet de virüsler var. Bunu MalwareBazaar sitesinden anlık olarak görebilirsiniz. Peki neden Linux kullanıcıları genelde bu virüslerden etkilenmiyor? Bunun en büyük nedeni Linux kullanıcılarının daha dikkatli olması[2] , Linux kullanıcılarının genellikle internetteki dosyalara ihtiyaç duymayıp her şeyi paket yöneticilerinden (örneğin, Flatpak, Snap, DEB, AUR, DNF vs.) indirmesi ve Linux virüslerinin çoğunluğunun masaüstü kullanıcılarını değil sunucuları hedeflemesi durumu göz önüne alındığında, "Linux Windows'dan daha güvenilir." demek yanlış mı? Aslında hayır. Çünkü Windows'un paket yöneticisinde ve Microsoft Store mağazasında çok az uygulama var ve bu yüzden genellikle kullanıcılar Windows kullanırken internetten uygulama yüklemek zorundalar. Paket yöneticisi ise internetteki uygulamalara göre çok daha güvenilir olduğundan dolayı Linux kullanıcıları hala Windows kullanıcılarından daha güvende.
    2. Konu ile ilgili önerdiğim video (Türkçe): Linux'da Virüs Yok Yalanı... (virüs yüklüyorum)

---

2 Windows kullanan kişiler genelde bilgisayarını aldığında Windows kurulu geldiği için öyle kullanıyor ve pek bilgileri yok. Fakat Linux'u öğrenen birisi, İnternet aleminin nasıl bir yer olduğundan haberdar ve bu yüzden daha dikkatliler.

Yazışma Güvenliği

Bu oldukça uzun bir konudur fakat bu yazıyı okuyanlar için en basit şekilde nasıl güvenli bir şekilde mesajlaşacağınızı size anlatayım.

1. Uçtan uca şifreleme koruması olan yazılımlar kullanın. (Uçtan uca şifreleme hakkında daha detaylı konuşacağız.)
    1. WhatsApp ve Facebook mesajlarınızın uçtan uca şifrelendiğini söyler fakat kaynak kodları gizli olduğundan asla bundan emin olamayız. Fakat Signal gibi açık kaynaklı uçtan uca şifreleme yapan uygulamalar da var. Zorunda kalmadıkça Signal kullanmanızı öneriyorum.
2. **SMS** ve **E-Posta** ile mesajlaşmayın.
    1. **SMS**: SMS Mesajlar zaten yapısı gereği asla güvenli olamaz. Detaylı bilgi için okuyabilirsiniz: Why SMS Text Messages Aren't Private or Secure - How-To Geek
    2. **E-Posta**: E-posta da SMS gibi güvenli olması pek mümkün değildir. Güvenli olması için kendi sunucunuzun olması gerekir ve mesajlaşacağınız kişinin de sizin sunucunuzun mailini kullanıyor olması gerekir. Aksi takdirde Gmail ya da hangi e-posta hizmetini kullanıyorsanız o sizin mesajlarınızı görebilecek. Siz kendi sunucunuzdan Gmail kullanan birisine mail attığınızda da mail ona gideceği ve onun da Gmail kullandığı için Google mesajlarınızı görebilecektir.

Uçtan uca şifreleme nedir? Nasıl çalışır?

Uçtan uca şifreleme, iletişimdeki mesajların gönderici cihazından alıcı cihazına kadar olan süreçte sadece gönderici ve alıcı tarafından okunabilecek şekilde şifrelendiği bir güvenlik protokolüdür. Bu şifreleme yöntemi, iletişim kanalı boyunca herhangi bir aracının (örneğin, sunucu veya ağ yönlendiricisi gibi) mesaj içeriğine erişememesini sağlar. İletişim kanalı üzerinde aktarılan bilgiler, sadece gönderici ve alıcı tarafından okunabilir hale gelir.

Mantık olarak, uçtan uca şifreleme işlemi şu adımlardan oluşur:

1. **Anahtar Oluşturma**: İletişimde bulunan her iki taraf için de birer anahtar oluşturulur. Bu anahtarlar, mesajların şifrelenmesi ve çözülmesi için kullanılacak şifreleme algoritmalarını belirler.
2. **Şifreleme**: Mesaj gönderici tarafından oluşturulduktan sonra, gönderici tarafından kullanılan anahtarlarla şifrelenir. Bu işlem, mesajın içeriğini anlamı hale gelmeyecek bir halde yapar.

3. **İletişim Kanalı**: Şifrelenmiş mesaj, internet veya diğer iletişim kanalları üzerinden alıcıya gönderilir. Bu aşamada, mesajın içeriği şifreli olduğundan, araya giren herhangi bir kişi mesajı okuyamaz veya anlayamaz.
4. **Çözme**: Alıcı, şifreli mesajı alır ve kendi anahtarını kullanarak mesajı çözer. Bu işlem sonucunda, mesajın orijinal içeriği alıcı tarafından okunabilir hale gelir.

Bu adımların tamamlanmasıyla, iletişim sürecindeki mesajlar sadece gönderici ve alıcı tarafından anlaşılabilir. Bu nedenle, üçüncü tarafların mesajları izlemesi veya okuması neredeyse imkansız hale gelir. Uçtan uca şifreleme, güvenli ve gizli bir iletişim sağlamak için yaygın olarak kullanılan etkili bir güvenlik önlemidir. Uçtan uca şifrelemeyi anlatmak zordur bu matematikçilerin işidir fakat matematik olmadan en basit şekilde anlatmak gerekirse böyle.

Ağ Güvenliği

Ağ Güvenliği, size internette gezerken nasıl güvenli olabileceğinizi öğretecektir.

Tarayıcınız

Tarayıcıları hepimiz biliyoruz. Bunlardan en çok bilinenleri Google Chrome, Opera, Brave ve Firefox. Peki ya en güvenli ve en gizli olanları hangileri?

Aşağıdaki listeden hangi tarayıcının daha gizli ve güvenli olduğu anlaşılacaktır.

Kriterler:

1. Tarayıcı açık kaynaklı mı? (Açık kaynak olması daha iyidir. Bunun sebebini üstte anlatmıştık)
2. Chromium tabanlı mı? (Tarayıcının Chromium tabanlı olması hem Chrome'yi tekel yapar hem de Özgür Web anlayışını bozar)
3. Yerleşik Betik (Script) Engelleyici var mı?
4. Reklam Engellemek mümkün mü?
5. Otomatik Çerez Engelleyici var mı? (Eklentisiz, ayar olarak)
6. Otomatik HTTPS yükseltme ayarı var mı? (Eklentisiz tabii ki)

Gizlilik ve Güvenlik testi:

Yerleşik Özellikler:	Brave	Firefox	Safari	Google Chrome	DuckDuckGo
Açık Kaynak mı?	Evet	Evet	Hayır	Hayır	Kısmi
Chromium Tabanlı mı?	Evet	Hayır	Hayır	Evet	Evet
Yerleşik Betik (Script) Engelleyici var mı?	Var	Var	Yok	Yok	Var
Reklam Engelleme	Var	Var	Yok	Eklentiler ile mümkün	Var
Otomatik Çerez Engelleme	Var	Yok	Var	Yok	Var
Otomatik HTTPS'ye yükseltme	Var	Var	Var	Var	Var

Sonuç:

Gizlilik ve Güvenlik için en iyi tarayıcılar (sırasıyla): **Brave**, **Firefox**, **DuckDuckGo**

Gizlilik ve Güvenlik için en iyi ve Chromium tabanlı olmayan tarayıcı: **Firefox**

Gizliliğinizi ve güvenliğinizi önemsiyorsanız asla kullanmamanız gereken tarayıcılar: **Safari**, **Google Chrome**

Peki Mobilde en iyi tarayıcı hangisidir? Hiç kuşkusuz **Firefox**.

Neden Firefox?

1. Mobilde en fazla eklenti destekliyor (sorunsuz bir şekilde)
2. Hem eklenti destekleyip hem de rakiplerine göre çok çok güvenli
3. Açık Kaynak Yazılım

Arama Motorunuz

Tarayıcınızdaki arama motorundan bir şey aradığınızda arama motorunu kullanıyorsunuz. Bu yüzden Arama Motorunuz da çok önemli.

Kriterler:

1. Çerez kullanıyor mu?
2. Arama kaydını tutuyor mu?
3. IP Adresleri kaydediyor mu?
4. Üçüncü taraflarla veri paylaşıyor mu?

Renklerin anlamları:

Yeşil: İyi

Kırmızı: Kötü

Gri: Hepsi yapıyor/normal

Arama Motoru Testi:

	Google	DuckDuckGo	Bing	Startpage
Çerezler	Çerezler kullanır	Çerezler kullanmaz	Çerezler kullanır	Çerezler kullanır
Arama Kaydı	Arama kaydını tutar	Arama kaydını tutmaz	Arama kaydını tutar	Arama kaydını tutmaz
IP Adresi Kaydı	IP adreslerini kaydeder	IP adreslerini kaydeder	IP adreslerini kaydeder	IP adreslerini kaydeder
Veri Paylaşımı	Üçüncü taraflarla paylaşır	Veri paylaşımı yapmaz	Üçüncü taraflarla paylaşır	Veri paylaşımı yapmaz

Sonuç:

Gizliliğe en çok önem veren arama motoru: **DuckDuckGo**

VPN:

VPN temel olarak size şunları sağlar;

- İletişiminizi cihazınız ile VPN sağlayıcınız arasında şifreleyerek gözetime, engele veya değiştirilmeye uğramasına engel olur.
- VPN'e bağlı olduğunuz sürece VPN sağlayıcınızın sunucusundan çıkış yapacağınız için girdiğiniz web siteleri veya kullandığınız hizmetler VPN IP adresinizi göreceğinden, kim olduğunuzu siz belirtmediğiniz sürece bilmeleri zorlaşacaktır.
- VPN kimi koşullar için yeterince anonimlik sağlamamakla beraber, eğer ortak bir VPN sunucusu kullanıyorsanız, bağlı olduğunuz VPN sunucusundaki herkes ile aynı IP adresini paylaştığınızdan kalabalığın içine karışmış olursunuz.

Neden VPN kullanmalıyım?

VPN kullanmak için çok çeşitli sebepleriniz olabilir;

- Bulunduğunuz ülkeden veya kullandığınız ağdan erişim kısıtlaması olan hizmetlere erişmek istiyorsunuzdur.
- Ağ üzerinden iletişiminizi denetleyen, takip eden, kaydeden kişilere karşı mahremiyetinizi korumak istiyorsunuzdur.
- Bağlı olduğunuz yerel ağ üzerinden size yöneltilebilecek saldırılara karşı korumaya ihtiyacınız vardır.

Ücretsiz VPN olur mu?

Türkiye'de ve dünyada yaşanan her engelleme ve sansür girişiminde akla ilk gelen çözüm VPN'dir. Neredeyse her tavsiye ise **bedava** VPN hizmetleri üzerinden yürür. Doğal olarak sansür durumunda VPN kullanan çoğu insanın, tek amacı sansürü aşarak ihtiyaç duyduğu bilgiye veya hizmete erişmek ve VPN teknolojisi hakkındaki bilgisi kısıtlı olduğundan, olası tehlikelerin üzerine düşünmediği söylenebilir. Bir VPN hizmet sağlayıcısı, sunucusuna bağlı olduğunuz sürece;

- Sizin IP adresinizi ve buna bağlı olarak konumunuzu bilebilir.
- Ziyaret ettiğiniz web sitelerini ve kullandığınız hizmetleri, içeriğini bilemese bile kaydedebilir.
- Şayet VPN istemcisi bir tarayıcı eklentisi şeklinde kurulduysa, kötücül bir eklenti tüm tarama verisine erişebilir.
- Dikkatli olunmazsa kötücül bir VPN sunucusu iletişimizin arasına girip verilerinizi çalabilir, size istenmeyen reklamlar sunabilir veya cihazınıza zarar vermeye çalışabilir.

Bu sebeplerden ötürü VPN kullanmak hizmet sağlayıcıya bir biçimde güven gerektirir. Daha doğru bir ifade ile VPN; **İnternet servis sağlayıcınıza olan güveninizi VPN sağlayıcınıza aktarır.** Nasıl ki evinizin anahtarını rastgele birine vermiyorsanız İnternet bağlantınızı da rastgele birinin eline vermemeniz gerekir. Bu sebepten ötürü İnternet hizmetlerine ilişkin **para vermiyorsanız ürün sizsiniz** sözüne dayanarak VPN'i satın almanız veya kendi sunucunuzu kurarak kullanmanız gerekir.

Bu duruma istisna sayılabilecek birkaç örnek bulunmakta. Bu istisnalar, dünyada mahremiyet ve dijital hak mücadelesi içinde olan toplulukların ücretsiz hizmetleri ve kimi güvenilir adledilen şirketin giriş seviyesi bedava verdikleri hizmetlerdir. Aşağıdaki liste dahilinde ücretsiz VPN sunan ve genel olarak güvenli görülen kurumları bulabilirsiniz.

Riseup

Calyx Institute

ProtonVPN

VPN hizmeti seçerken dikkat edilmesi gerekenler:

- **Özgür yazılım** kullanmayan hiç bir VPN sağlayıcıya güvenmeyin. VPN ile tüm ağ trafiğinizi teslim ettiğiniz bir şirketin kullandığı yazılımların sizin özgürlüğünüze karşı olması hiç güven telkin eden bir unsur değildir.
- Kayıt tutmama politikası pek çok VPN servisinin iddiasıdır. Bu, sunucularına yapılan bağlantılara ilişkin kayıtların hiç tutulmadığını ifade eder. Elbette geçmişte bunun sadece bir iddia olduğu ve doğrulanamayacağını gösteren sözünü tutmamış VPN şirketleri vardır. Bazı hizmet sağlayıcılar sunucularında sabit sürücü bile bulundurmadıklarını ifade etmektedir. Bu konuda diğer konularda olduğu gibi VPN sağlayıcının sözüne güvenmek zorunluluğu olduğundan daha önce devletlere bilgi sağlayıp sağlamadığına bakılması önemli olabilir. PureVPN vakası bu konuda incelenmeye değer bir örnek. Daha sonra VPN sağlayıcının geçmişini, kaç yıldır hizmette olduğunu ve birinci elden, bağımsız kullanıcı deneyim ve yorumlarını okumak faydalıdır.
- VPN sağlayıcınızın özgür yazılım olan OpenVpn desteklediğinden ve yapılandırma (config) dosyalarını sizinle paylaştığından emin olun. Bu sayede GNU/Linux ve Android işletim sistemine sahip cihazlarınızda kolaylıkla yerleşik VPN istemcilerini kullanabilirsiniz. Bu imkan aynı zamanda VPN sağlayıcının yazılımına mahkum kalmamanızı da garanti eder.
- ABD, Birleşik Krallık ve Almanya gibi ülkelerin Internet kullanıcılarını gözetlemek ve profillemek için çokça çabaya giriştiği ve yasal(!) imkanları kullanarak pek çok şirketten zorla veri aldığı bilinmektedir. Bu bakımdan

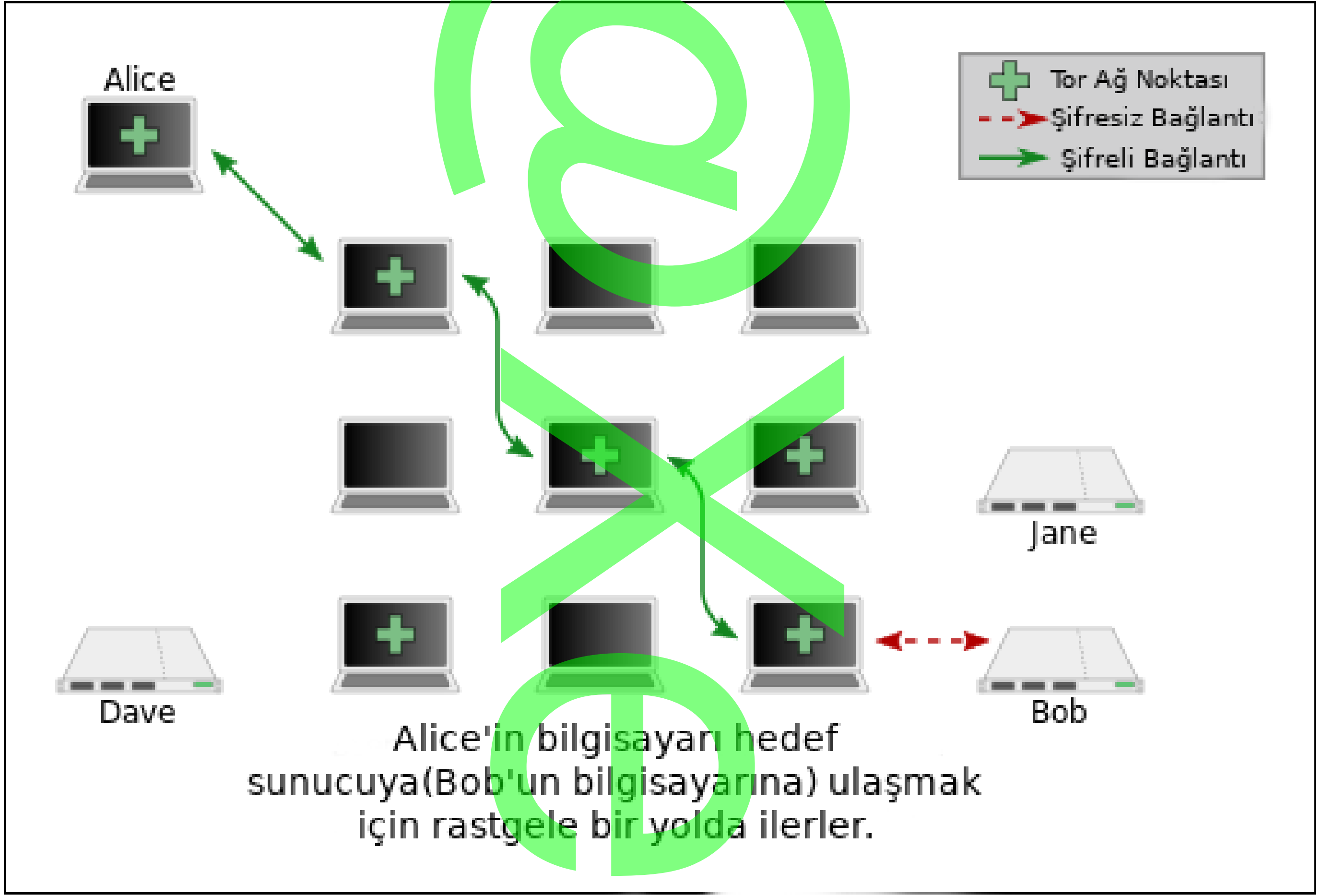
VPN sağlayıcınızın bu konuda kötü bir geçmişi olmayan ve hukuki güvenlik bakımından iyi sayılan ülkelerden seçmeniz kesinlikle tavsiye edilir. Hollanda veri merkezlerinin hızından dolayı, İsviçre'de AB hukuk sisteminin dışında ve mahremiyet yanlısı sağlam hukuk sisteminden dolayı tercih edilmektedir.

- VPN sağlayıcınızın mutlaka bağlantı için farklı protokollere izin verdiğinden emin olun. Çoğu VPN engellemesi standart portlar ve protokollere yönelir. Şayet elinizde geniş bir bağlantı imkanı olursa bu tip yasakları aşmanız kolaylaşacaktır. Bunlar arasında en önemlileri SSL tünelleme, SSH tünelleme yer almaktadır.
- Herhangi bir bağlantı kısıtlaması özgürlüğünüze karşı bir harekettir. Bu bakımdan bir VPN sağlayıcı sizin torrent kullanmanıza veya indirme hızınıza karışıyorsa hem bir çeşit kayıt tutuyordur hem de bağlantı özgürlüğünüzü sınırlıyordur.
- Bir VPN sağlayıcı sizden kayıt için hiç bir kişisel veri talep etmemelidir. Buna ödeme imkanları arasında kriptoparalar ve posta yolu ile nakit gönderimi gibi anonim seçenekler bulundurmak da dahildir. Nihayetinde VPN sağlayıcınıza güveniyor olacaksınız kimliğiniz için fakat şirkete güvenseniz bile devletler ve kötücül saldırıların ihtimali hala asgari veriyi teslim etmeniz için geçerli gerekçelerdir.

Tor:

Tor ağı nasıl çalışır?

Tor ağının başlıca amacı; kullanıcılarının internet üzerindeki kimliklerini ve aktivitelerini ağ trafiğini rastgele bağlantı noktaları üzerinden sektirerek her türlü otorite gözetiminden korumaktır.



Alice'in bilgisayarı hedef sunucuya(Bob'un bilgisayarına) ulaşmak için rastgele bir yolda ilerler.

Her bağlantı noktasını bir kaldırım taşı olarak düşünürseniz, Tor ağı sizin ve bağlanmak istediğiniz hedefin arasında rastgele kaldırım taşlarından oluşturulmuş bir yol yaratır. Böylelikle sizden çıkan trafiğin nereye gittiği veya karşıdan gelen bilginin kime geldiğini sadece giriş ve çıkış noktaları bilebilir. (Bu aynı zamanda Tor ağının bir zayıflığıdır ve ileriki başlıklarda değinilecektir.)

Buraya kadar genel işleyişi anlayıp benimsediyseniz yavaş yavaş tarayıcı kurulumuna geçebiliriz.

Tor Browser

Öncelikle şunu asla unutmayın, Tor Browser bilgisayarınızın tüm trafiğini Tor ağı üzerinden **geçirmez.**
Örneğin, Tor Browser ile gezinirken, arkaplanda "X" bir mesajlaşma programı kullanıyorsanız, "X" programı üzerinden giden trafik Tor'dan geçmeyecek, dolayısıyla anonim olmayacaktır.

Tor Browser, Mozilla Firefox'un bir çatallamasıdır (fork).

Ülkemizde Tor ağının bilinen düğümleri engellenmiş durumda olduğundan Tor ağına köprüleri (bridges) kullanarak bağlanabiliyoruz.

Türkiye'de Tor yasaklı DEĞİLDİR, çünkü "Tor'u yasaklamak" diye bir şey YOKTUR.

Gönüllü olarak işletilen Tor düğümlerinin IP adresleri İnternet'te açık bir şekilde listelenmektedir. Böylelikle otoriteler (kurumlar, kuruluşlar veya devletler) bu IP adreslerini bloklayarak Tor ağına erişim engellemeye çalışmaktadır. Ancak bu durum Tor'u tamamen erişilemez hale getiremez. Tor'un engellenmeye çalışıldığı ülkelerde Tor'a erişim, **köprüler** aracılığıyla gerçekleşir. Bu köprüler, Tor Project'in web sitesinde bahsedildiği üzere, ana Tor dizininde bulunmazlar. Halka açık olarak yayınlanan bir liste bulunmadığından otoritelerin bütün bu IP adreslerini bulup engellemesi neredeyse imkansızdır.

Köprü kullanarak Tor ağına girmeye çalıştığınızda, öncelikle her zamanki gibi halka açık bir Tor düğümüne değil, bir köprüye bağlanırsınız. Daha sonra bağlandığınız köprü sizi şifreli bir bağlantı ile halka açık bir Tor ağ noktasına bağlar ve böylelikle Tor ağına girişiniz gerçekleşmiş olur.

Tor Browser'ı, Tor'un kendi web sitesi Türkiye'de erişime engelli olduğu için EFF Tor yansısından indirebilirsiniz.

Alternatif linkler:

- GitHub
- Archive.org
- Google Drive (mahremiyetinize saygı göstermez)

Bunların hiçbirine erişemiyorsanız, gettor@torproject.org adresine, işletim sisteminizi ve istediğiniz dili içeren aşağıdaki gibi bir e-posta atarsanız, indirme linkiniz attığınız e-postaya cevap olarak gelecektir. *Cevabın gelmesi bazen 1 saati bulabilmektedir.*

Daha detaylı bilgiler için okuyunuz:

https://guvenlik.oyd.org.tr/ag_guvenligi/tor.html

Mac Adresi Değişikliği

MAC adresi ağ aygıtlarını eşsiz şekilde tanımlayan bir kimlik bilgisidir. Yönlendiriciler gibi ağ aygıtlarının ağda bulunan cihazları birbirinden ayırmasına ve paketleri doğru istemcilere yönlendirmesine imkan sağlamaktadır. Lakin kullanıcıya ve cihaza ait her eşsiz değer gibi bağlanılan ağları kontrol edenler veya WiFi sinyallerini inceleyebilenler için bir takip imkanı da ortaya çıkarmakta.

Bu sebepten ağ bağlantısı kuran ve özellikle bunu kablosuz gerçekleştiren cihazlar için MAC adresinizin gerekmedikçe aynı kalmaması sizin takip edilme ihtimalinizi azaltacaktır.

MAC adresi ağ aygıtlarının sunduğu hizmetlerin çalışması için de gerekli. Şayet bağlandığınız ağın sizi yetkilendirme veya Captive Portal gibi sebeplerden tanıması gerekiyorsa MAC adresinizi değiştirmeniz bu yetkilendirmeyi ortadan kaldıracağından hangi ağlarda bunu yapmak istediğinize dikkatli karar vermeniz gereklidir.

GNU/Linux

GNU/Linux'da MAC adresi değiştirmek için macchanger adlı pakete ihtiyacınız olacak. Çoğu dağıtımda dahili olarak gelmediğinden aşağıdaki komutlarla kurabilirsiniz.

Debian tabanlı dağıtımlar için: sudo apt-get install macchanger

RPM tabanlı dağıtımlar için: sudo yum install macchanger

Macchanger bir komut satırı yazılımı olduğundan uçbirimden kullanmanız gerekecek.

macchanger --help komutu size aşağıdaki çıktıyı verecektir.

```
GNU MAC Changer
Usage: macchanger [options] device

  -h,  --help                   Print this help
  -V,  --version                Print version and exit
  -s,  --show                   Print the MAC address and exit
  -e,  --ending                 Don't change the vendor bytes
  -a,  --another                Set random vendor MAC of the same kind
  -A                            Set random vendor MAC of any kind
  -p,  --permanent              Reset to original, permanent hardware MAC
  -r,  --random                 Set fully random MAC
  -l,  --list[=keyword]         Print known vendors
  -b,  --bia                    Pretend to be a burned-in-address
  -m,  --mac=XX:XX:XX:XX:XX:XX
       --mac XX:XX:XX:XX:XX:XX  Set the MAC XX:XX:XX:XX:XX:XX

Report bugs to https://github.com/alobbs/macchanger/issues
```

Buradaki önemli parametreler ve işlevleri şu şekilde:

- --another: Cihazınızda tanımlı olan MAC adresine benzer yeni bir MAC adresi üretir.
- --permanent: Cihazınızın MAC adresini orjinal MAC adresine döndürür.
- --random: Tamamen rastgele bir MAC adresi oluşturur.
- --bia: Cihazın MAC adresinin değiştirildiğini belli etmez.
- --ending: Cihazın markasına uygun MAC adres oluşturur.

Macchanger ile işlem yapmadan önce cihazınızla ilgili iki işlem daha yapmanız gerekli. Bunlardan ilki MAC adresini değiştireceğiniz aygıtın adını öğrenmek diğeri de ağ aygıtlarını kapatmak.

Aygıt adını öğrenmek

Ağ aygıtınızın adını öğrenmek için neredeyse her dağıtımda ip a komutunu kullanabilirsiniz. Aşağıdaki gibi bir çıktı alacaksınız:

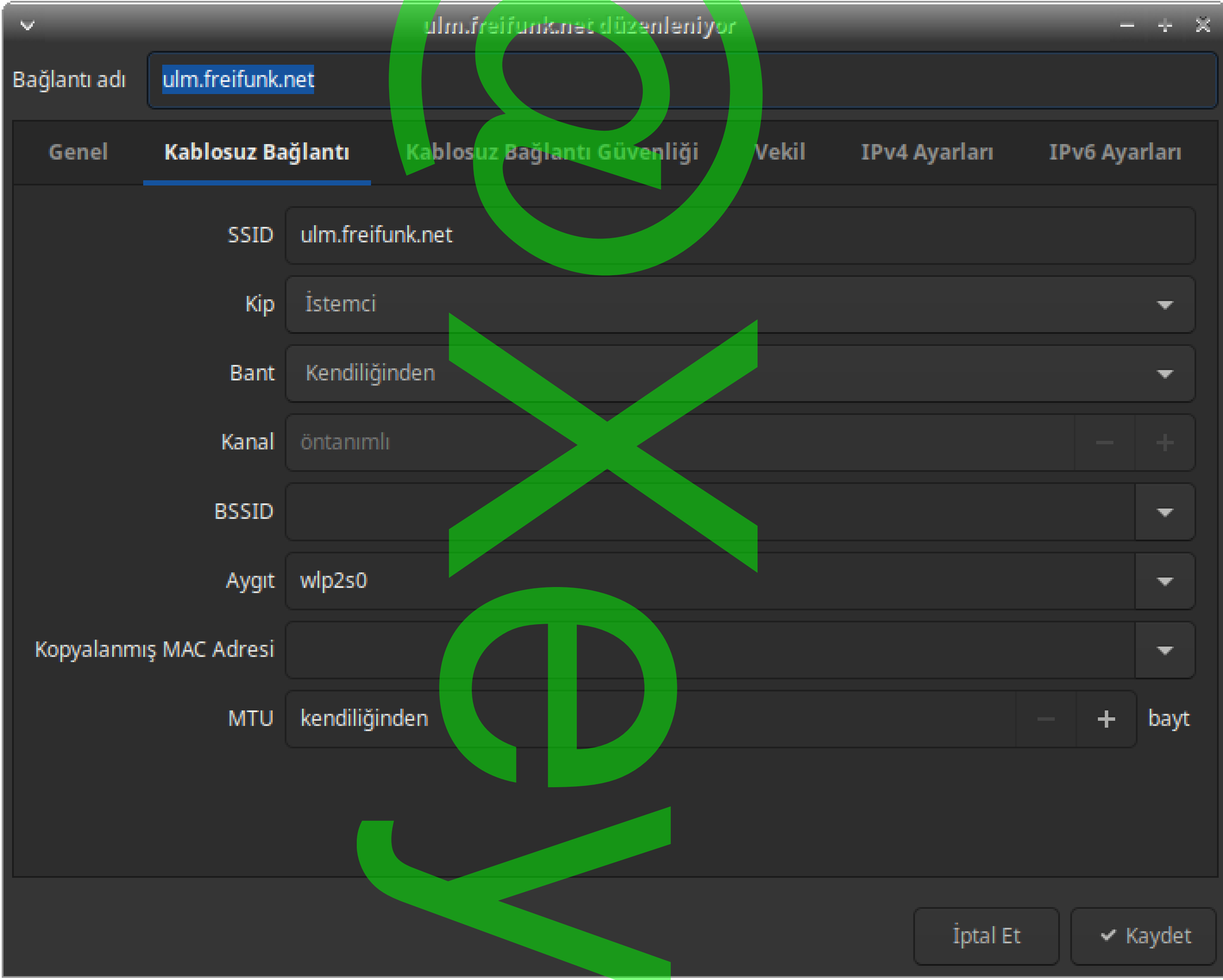
```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
     valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
     valid_lft forever preferred_lft forever
2: enp0s25: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel
state DOWN group default qlen 1000
   link/ether xx:xx:xx:xx:xx:xx brd ff:ff:ff:ff:ff:ff
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
state UP group default qlen 1000
   link/ether xx:xx:xx:xx:xx:xx brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.105/24 brd 192.168.1.255 scope global dynamic noprefixroute
wlp2s0
     valid_lft 85820sec preferred_lft 85820sec
   inet6 fde8:342f:910a:0:b98d:52b:15b8:8b9/64 scope global temporary dynamic
     valid_lft 86389sec preferred_lft 14389sec
   inet6 fde8:342f:910a:0:4e81:87ba:a068:4f7e/64 scope global dynamic
mngtmpaddr noprefixroute
     valid_lft 86389sec preferred_lft 14389sec
   inet6 fe80::3726:985a:a2e5:5509/64 scope link noprefixroute
     valid_lft forever preferred_lft forever
```

Bu çıktı karmaşık görünebilir ama iki parametreye ihtiyaç olacak basitçe.

2. numarada enp0s25 isimli aygıt kablolu ağ aygıtının adı.
3. numaradaki wlp2s0 isimli aygıt ise kablosuz ağ aygıtının adı.

Basitçe nmcli komutu dağıtımınızda mevcutsa size daha derli toplu bir çıktı verecektir.

Şayet uçbirim ile uğraşma istemiyorsanız dağıtımınızın ayarlarına girip ağ aygıtlarını seçip detaylarını incelediğinizde aygıtın adını orada da bulabilirsiniz.



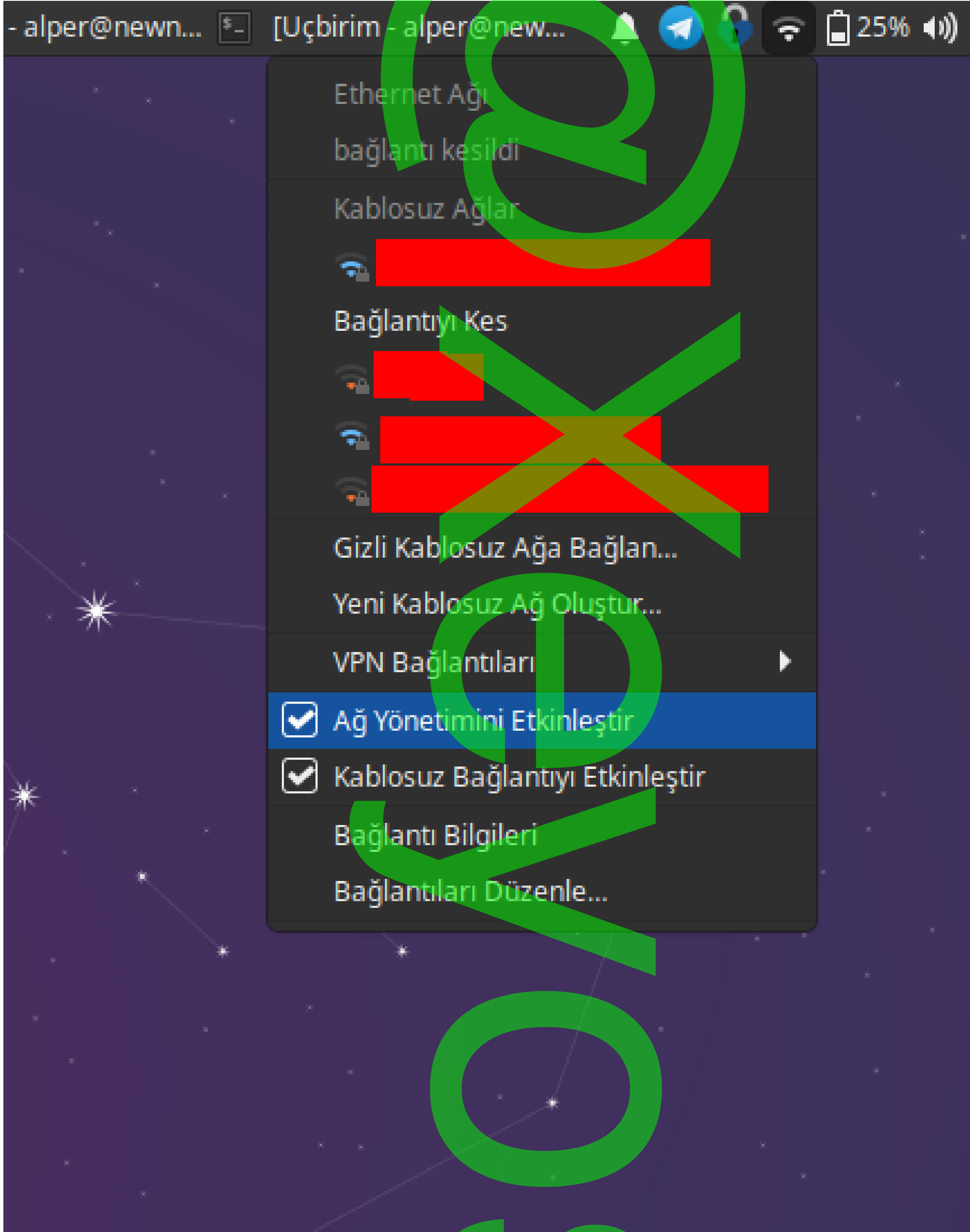
Ağ aygıtını devre dışı bırakmak

Hangi aygıtın MAC adresini değiştireceğinize karar verdikten sonra değiştireceğiniz aygıtın devredışı bırakılması gerekiyor. Bunu uçbirimden yapmak isterseniz aşağıdaki komutu kullanabilirsiniz:

Wifi'ı devredışı bırakmak için: nmcli radio wifi off

Tüm ağı devredışı bırakmak için: nmcli networking off

Bu işlemi de uçbirimden yapmak istemiyorsanız dağıtımınızın ağ ayarlarından hem WiFi hem de ağ aygıtlarının tamamını devredışı bırakabilirsiniz.



MAC adresi değiştirmek

MAC adresini tamamen rastgele değiştirmek en iyi seçeneklerden biri olacaktır. Bunun için aşağıdaki komutu kullanabilirsiniz.

sudo macchanger --random [ağ aygıt adı]

Şayet işlem başarılı olursa aşağıdaki çıktıyı alacaksınız:

Current MAC: 1a:0d:33:53:bf:97 (Samsung Electronics Co.,LTD)
Permanent MAC: 1a:0d:33:53:bf:97 (Samsung Electronics Co.,LTD)
New MAC: 86:40:e5:7b:3e:c1 (unknown)

Bu noktada `--bia` ve `--ending` parametrelerini ekleme kararı alınabilir. Bu durum tamamen içinde bulunduğunuz koşulun gerekliliklerine bağlı.

Orijinal MAC adresine geri dönmek

Bunun için basitçe aşağıdaki komutu çalıştırabilirsiniz:

```
sudo machanger --permanent [ağ aygıtı]
```

Android

Modern Android cihazlar wifi kartının MAC adresini rastgele değiştirme seçeneğine hali hazırda sahipler. Bu seçeneği Ayarlar > Ağ ve internet > Kablosuz > ağ ismi > Gelişmiş > Gizlilik altında bulabilirsiniz. Tamamen rastgele MAC adresi seçeneğini seçerseniz cihazınız seçtiğiniz ağa her bağlandığında yeni bir MAC adresi kullanacaktır.

Şimdilik bitti..

Eğer okuyup yararlandıysanız ne mutlu. Bu tür güvenlik ile ilgili rehberler ve e-kitaplar için Discord'dan bana ulaşabilirsiniz: @xeyossr